

# OPTIMAL MEASUREMENTS FOR THE DIHEDRAL HIDDEN SUBGROUP PROBLEM

DAVE BACON, ANDREW M. CHILDS, AND WIM VAN DAM

**ABSTRACT.** We consider the dihedral hidden subgroup problem as the problem of distinguishing hidden subgroup states. We show that the optimal measurement for solving this problem is the so-called pretty good measurement. We then prove that the success probability of this measurement exhibits a sharp threshold as a function of the density  $\nu = k/\log_2 N$ , where  $k$  is the number of copies of the hidden subgroup state and  $2N$  is the order of the dihedral group. In particular, for  $\nu < 1$  the optimal measurement (and hence any measurement) identifies the hidden subgroup with a probability that is exponentially small in  $\log N$ , while for  $\nu > 1$  the optimal measurement identifies the hidden subgroup with a probability of order unity. Thus the dihedral group provides an example of a group  $\mathcal{G}$  for which  $\Omega(\log |\mathcal{G}|)$  hidden subgroup states are necessary to solve the hidden subgroup problem. We also consider the optimal measurement for determining a single bit of the answer, and show that it exhibits the same threshold. Finally, we consider implementing the optimal measurement by a quantum circuit, and thereby establish further connections between the dihedral hidden subgroup problem and average case subset sum problems. In particular, we show that an efficient quantum algorithm for a restricted version of the optimal measurement would imply an efficient quantum algorithm for the subset sum problem, and conversely, that the ability to quantum sample from subset sum solutions allows one to implement the optimal measurement.

## 1. INTRODUCTION

Quantum computers promise to solve certain problems asymptotically faster than their classical counterparts. In particular, Shor's discovery of an efficient quantum algorithm for factoring [45]—a cryptographically significant task for which no efficient classical algorithm is known—has motivated considerable investigation into the potential algorithmic uses of quantum computers. Along with its predecessors [3, 8, 9, 46], Shor's algorithm can be viewed as a solution to one of a large class of problems known as *hidden subgroup problems* [4, 28], several of which also have applications to interesting computational problems for which no efficient classical algorithm is known. Thus the broader question arises: under what circumstances can the hidden subgroup problem (HSP) be solved efficiently by a quantum computer?

Encouragingly, the quantum query complexity of the general HSP is polynomial: for any group  $\mathcal{G}$ , only  $\text{poly}(\log |\mathcal{G}|)$  quantum queries of the function

that hides a subgroup are sufficient to solve the problem [12–15, 28]. Thus lower bounds showing that the HSP is intractable are unlikely to be forthcoming. However, the processing of the queries could take exponential time, so it remains a challenge to find algorithms that are efficient in terms of the number of elementary operations.

Following Shor’s discovery, there has been considerable progress in showing that quantum computers can efficiently solve the HSP for particular groups and particular kinds of subgroups [4, 17, 20–24, 29, 31, 33, 36, 43] (although there is also evidence that some hidden subgroup problems may be hard even for quantum computers [32, 37, 38]). However, for many hidden subgroup problems, the speedup offered by quantum computers (if any) remains unknown. In particular, no efficient quantum algorithm is known for two cases whose applications are of particular interest, the symmetric group and the dihedral group. For the former, an efficient quantum algorithm could be used to efficiently solve the graph isomorphism problem [2, 4, 12, 27], while for the latter, an efficient quantum algorithm could be used to efficiently solve certain cryptographically significant lattice problems [41]. Recent progress on the dihedral HSP has been particularly encouraging: Kuperberg gave an algorithm using subexponential (but superpolynomial) time and space [34], and Regev improved this algorithm to use a similar amount of time but only polynomial space [40].

In this paper we concentrate on the dihedral hidden subgroup problem. In particular, we study the optimal measurement for solving this problem given samples of certain quantum states we call *hidden subgroup states*. We find that the success probability of the optimal measurement exhibits a sharp threshold as a function of  $k$ , the number of copies of the hidden subgroup state. For the dihedral group of order  $2N$ , let  $k = \nu \log N$ , where  $\nu$  is the *density*. (The logarithms in this article are always base 2.) For any fixed density  $\nu > 1$ , the optimal measurement identifies the hidden subgroup with constant probability, and therefore an efficient quantum circuit for implementing this measurement would solve the dihedral hidden subgroup problem. (This can be compared to previous results showing that a success probability of  $1 - 1/2N$  can be achieved with  $\nu > 89$  [15], and that a success probability of  $1/\text{poly}(\log N)$  can be achieved with  $\nu > 1$  [41].) However, for any fixed  $\nu < 1$ , the success probability of the optimal measurement (and hence of any measurement) is exponentially small in  $\log N$ . This bound shows that  $\Omega(\log |\mathcal{G}|)$  hidden subgroup states are in fact necessary to solve the dihedral HSP. To the best of our knowledge this is the first time more than a constant number of copies of the hidden subgroup state have been shown to be necessary for any hidden subgroup problem.

In addition to studying the success probability of the optimal measurement, we also establish further connections between the dihedral hidden subgroup problem and average-case subset sum problems of density  $\nu$ . Regev showed that the dihedral HSP can be solved efficiently if one can efficiently solve average case subset sum problems with  $\nu > 1$  [41]. We show that the

optimal measurement for  $k = \nu \log N$  copies can be implemented if one can quantum sample from subset sum solutions at density  $\nu$ , and conversely, that an implementation of the optimal measurement (of a certain restricted form) by a quantum circuit can be used to solve the average case subset sum problem.

Our results can be compared to those of Ip showing that Shor's algorithm is an optimal solution to the abelian hidden subgroup problem [30]. In light of this observation, it is natural to consider the optimal measurement for other hidden subgroup problems as an approach to finding efficient algorithms. Our results show that if such an algorithm is efficient for the dihedral HSP, then one should focus on finding an efficient quantum algorithm for the average case subset sum problem with  $\nu > 1$  (or on implementing the measurement by a quantum circuit not of the restricted form that could be used to solve subset sum).

This paper is organized as follows. In Section 2, we review the hidden subgroup problem in general, and in Section 3, we review the dihedral hidden subgroup problem in particular. We present the optimal measurement for the dihedral HSP in Section 4 and establish bounds on its success probability in Section 5. In Section 6, we show that the bounds of Section 5 are significantly stronger than those one obtains from straightforward information-theoretic arguments. Then, in Section 7, we show that the problem of determining just the least significant bit of the answer requires essentially as many copies of the hidden subgroup state as are required to obtain the entire answer. In Section 8, we establish connections between the optimal measurement for the dihedral HSP and the subset sum problem. Finally, we conclude in Section 9 with a discussion of the results and some open problems.

## 2. THE HIDDEN SUBGROUP PROBLEM

We begin by reviewing the hidden subgroup problem. Let  $\mathcal{G}$  be a finite group of order  $|\mathcal{G}|$ . We assume that the elements of this group can be efficiently represented as strings of  $\text{poly}(\log |\mathcal{G}|)$  bits. Consider a function  $f : \mathcal{G} \rightarrow S$  where  $S$  is some finite set whose elements can also be efficiently represented as strings of  $\text{poly}(\log |\mathcal{G}|)$  bits. In the HSP, we are given such a function and promised that it is constant and distinct on left cosets of some subgroup  $\mathcal{H} \leq \mathcal{G}$ . In other words,  $f(g_1) = f(g_2)$  if and only if  $g_1$  and  $g_2$  are in the same left coset of  $\mathcal{H}$ . The hidden subgroup problem is, given the ability to query the function  $f$ , to produce a generating set for the subgroup  $\mathcal{H}$ .

In the quantum version of the HSP we are given a unitary operator  $U_f$  that computes the function  $f$ . Explicitly, this quantum oracle acts as

$$(1) \quad U_f : |g, y\rangle \mapsto |g, y \oplus f(g)\rangle$$

for all  $g \in \mathcal{G}$  and  $y \in S$ , where  $\oplus$  is the bitwise exclusive or operation. If we input the basis state  $|g, 0\rangle$  into this oracle, it simply evaluates the function:

$U_f|g, 0\rangle = |g, f(g)\rangle$ . Our goal is to use this black box to find generators of the hidden subgroup in a time polynomial in  $\log |\mathcal{G}|$ .

In the standard approach to solving the hidden subgroup problem with a quantum computer (used by all known quantum algorithms for the HSP), one inputs a superposition over all group elements into the first register and  $|0\rangle$  into the second register, giving

$$(2) \quad U_f : \frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} |g, 0\rangle \mapsto \frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} |g, f(g)\rangle.$$

Suppose we now discard the second register. Due to the promise on  $f$ , the state of the first register is then a mixed state whose form depends on the hidden subgroup  $\mathcal{H}$ ,

$$(3) \quad \rho_{\mathcal{H}} := \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{g \in \mathcal{K}} |g\mathcal{H}\rangle \langle g\mathcal{H}|$$

where  $\mathcal{K} \subset \mathcal{G}$  is a complete set of left coset representatives of  $\mathcal{H}$  in  $\mathcal{G}$  (of size  $|\mathcal{K}| = |\mathcal{G}|/|\mathcal{H}|$ ), and where we have defined the coset states

$$(4) \quad |g\mathcal{H}\rangle := \frac{1}{\sqrt{|\mathcal{H}|}} \sum_{h \in \mathcal{H}} |gh\rangle.$$

We will call  $\rho_{\mathcal{H}}$  the *hidden subgroup state* corresponding to the subgroup  $\mathcal{H}$ .

Early quantum algorithms, including Deutsch's algorithm [9], the Deutsch-Jozsa algorithm [8], the Bernstein-Vazirani algorithm [3], Simon's algorithm [46], and Shor's algorithm [45], all solve examples of the abelian HSP but were not originally described in this language. The formulation in terms of a hidden subgroup was presented by Boneh and Lipton [4], who also noted the connection between the HSP over the symmetric group and the graph isomorphism problem.

The HSP over arbitrary finite abelian groups has an efficient quantum algorithm [4, 23, 33, 45, 46]. Hallgren, Russell, and Ta-Shma proved that the HSP has an efficient quantum algorithm whenever the subgroup  $\mathcal{H}$  is promised to be normal and there is an efficient quantum Fourier transform over the group  $\mathcal{G}$  [24]. Grigni, Schulman, Vazirani, and Vazirani showed that the HSP over "almost abelian" groups has an efficient quantum solution [21], and this result was extended by Gavinsky to "near-Hamiltonian" groups [20]. Püschel, Rötteler, and Beth gave an efficient quantum algorithm for the HSP over the wreath product  $\mathbb{Z}_2^n \wr \mathbb{Z}_2$  [43], and Friedl et al. showed how to solve the HSP over a semidirect product  $\mathbb{Z}_{p^k}^n \rtimes \mathbb{Z}_2$  for a fixed prime power  $p^k$  [17]. Moore, Rockmore, Russell, and Schulman gave an efficient quantum algorithm for the HSP over certain semidirect product groups, the  $q$ -hedral groups [36], and Inui and Le Gall gave a solution for semidirect product groups of the form  $\mathbb{Z}_{p^k} \rtimes \mathbb{Z}_p$  with  $p$  an odd prime [29].

Finally, as mentioned in the introduction, there is also a body of knowledge about the query complexity of the HSP. In particular, Ettinger, Høyer,

and Knill have shown that  $O(\log |\mathcal{G}|)$  quantum queries of the function  $f$  are sufficient to determine the hidden subgroup [13]. Unfortunately, the quantum algorithm they present requires time  $O(|\mathcal{G}|)$ .

### 3. THE DIHEDRAL HIDDEN SUBGROUP PROBLEM

The dihedral group of order  $2N$ , denoted  $\mathcal{D}_N$ , is the group of symmetries of a regular  $N$ -sided polygon. This group is generated by two elements  $r$  and  $s$  satisfying the relations  $r^2 = e$ ,  $s^N = e$ , and  $rsr = s^{-1}$ , where  $e$  is the identity element. Here  $s$  corresponds to a rotation of the polygon and  $r$  corresponds to a reflection. A generic element of the dihedral group can be written as  $r^t s^k$  where  $t \in \mathbb{Z}_2$  and  $s \in \mathbb{Z}_N$ , and group multiplication is given by  $r^{t'} s^{k'} r^t s^k = r^{t+t'} s^{k+(-1)^t k'}$ . (Throughout this article we write  $\mathbb{Z}_N$  to denote  $\mathbb{Z}/N\mathbb{Z}$ .)

The dihedral hidden subgroup problem (DHSP) was first considered by Ettinger and Høyer [15]. They showed that given  $O(\log N)$  queries to the hidden subgroup oracle for the dihedral group, there exists a quantum algorithm whose output contains enough classical information to solve the DHSP, and therefore that the query complexity of the DHSP is  $O(\log N)$ . Unfortunately, they were not able to find an efficient algorithm to process the output, so this approach has not yet led to an efficient algorithm for the DHSP.

A major motivation for attempting to solve the DHSP is a connection to lattice problems discovered by Regev [41]. A  $d$ -dimensional lattice is the set of all integer linear combinations of  $d$  linearly independent vectors in  $\mathbb{R}^d$  that form a basis for the lattice. In the *shortest vector problem*, one attempts to find the shortest (nonzero) vector in the lattice given a basis. In particular, in the  $g(d)$  *unique shortest vector problem*, we are promised that the shortest vector is unique and shorter than all other non-parallel vector by a factor  $g(d)$ . The presumed hardness of certain  $g(d)$  unique shortest vector problems is the basis for a cryptosystem proposed by Ajtai and Dwork (in which  $g(d) = O(d^8)$ ) [1], and a subsequent improvement proposed by Regev (in which  $g(d) = O(d^{1.5})$ ) [42]. Regev showed that an efficient quantum algorithm for the DHSP that works by sampling hidden subgroup states can be used to solve the  $\text{poly}(d)$  unique shortest vector problem [41], thereby breaking the proposed lattice cryptosystems.

Regev also gave a promising path toward solving the DHSP in the form of a connection to the *subset sum problem*. In the subset sum problem, one is given  $k$  numbers between 0 and  $N - 1$ , denoted  $x \in \mathbb{Z}_N^k$ , and a target  $t \in \mathbb{Z}_N$ , and the goal is to find a subset of the  $k$  numbers, specified by a binary vector  $b \in \mathbb{Z}_2^k$ , such that  $b \cdot x = t$ , where  $b \cdot x := \sum_{j=1}^k b_j x_j \bmod N$ . If such a subset exists, then we call  $(x, t)$  a legal subset sum input. Regev has shown that if one can efficiently solve  $1/\text{poly}(\log N)$  of the legal subset sum inputs (with  $k > \log N + 4$ ) then there is an efficient quantum algorithm for the DHSP [41]. While the general subset sum problem is NP-hard, note

that an algorithm for average-case inputs with  $k > \log N + 4$  a fixed function of  $N$  would be sufficient to solve the DHSP.

The first subexponential time quantum algorithm for the DHSP was given by Kuperberg, who showed how to solve it in  $2^{O(\sqrt{\log N})}$  time, space, and queries [34]. Regev reduced the space requirement to  $\text{poly}(\log N)$  at the expense of only slightly greater time and queries [40]. Regev's approach also shows a connection to the average case subset sum problem.

In trying to solve the DHSP, it is convenient to focus on a simplified version that is in fact equivalent in difficulty to the full problem. Specifically, we will focus on the case in which the subgroup  $\mathcal{H}$  has order two. In general, there are two types of subgroups of  $\mathcal{D}_N$ , cyclic subgroups and dihedral subgroups. The cyclic subgroups consist only of rotations; they are of the form

$$(5) \quad \mathcal{C}_{N/j} := \{e, s^j, \dots, s^{-j}\},$$

where  $j \in \mathbb{Z}_N$  is a divisor of  $N$ . Note that  $\mathcal{C}_1$  is simply the trivial subgroup. The dihedral subgroups consist of rotations and reflections, and are of the form

$$(6) \quad \mathcal{D}_{N/j,d} := \{e, s^j, \dots, s^{-j}, rs^d, rs^{j+d}, \dots, rs^{-j+d}\},$$

where  $j \in \mathbb{Z}_N$  is a divisor of  $N$  and  $d \in \mathbb{Z}_N$ . Note that  $\mathcal{D}_{N,d} = \mathcal{D}_N$  for any  $d$ . Furthermore, note that  $\mathcal{D}_{1,d} = \{e, rs^d\}$  is an order two subgroup for any  $d$ . The cyclic subgroups  $\mathcal{C}_{N/j}$  are all normal in  $\mathcal{D}_N$  (that is,  $ghg^{-1} \in \mathcal{C}_{N/j}$  for all  $h \in \mathcal{C}_{N/j}$  and  $g \in \mathcal{D}_N$ ) while none of the dihedral subgroups are normal except for the full dihedral group,  $\mathcal{D}_N$ .

Ettinger and Høyer have shown that an efficient quantum algorithm for the DHSP exists if one can solve the DHSP with the promise that the hidden subgroup is either the trivial subgroup,  $\mathcal{C}_1 = \{e\}$ , or is some subgroup of order two,  $\mathcal{D}_{1,d} = \{e, rs^d\}$  for some (unknown)  $d \in \mathbb{Z}_N$  [15]. We will further restrict the problem by determining the optimal measurement only for the order two subgroups. In fact, it will turn out that when this restricted measurement succeeds with high probability, it also identifies the trivial subgroup with high probability, and therefore can be used to solve the DHSP in general.

We will represent a dihedral group element  $r^t s^k$  using two quantum registers,  $|t, k\rangle$ , where the first register is a single qubit and the second register consists of  $\lceil \log N \rceil$  qubits. When the subgroup is an order two subgroup  $\mathcal{D}_{1,d}$ , then the standard approach produces the random coset state

$$(7) \quad |\phi_{k,d}\rangle = \frac{1}{\sqrt{2}}(|0, k\rangle + |1, -k + d\rangle)$$

where  $k$  is uniformly sampled from  $\mathbb{Z}_N$  and addition is done in  $\mathbb{Z}_N$ , i.e., modulo  $N$ . In other words, the hidden subgroup state corresponding to the

subgroup  $\mathcal{H} = \mathcal{D}_{1,d}$  is

$$(8) \quad \rho_d = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} |\phi_{k,d}\rangle \langle \phi_{k,d}|.$$

It will be convenient to change the basis by Fourier transforming the second register (over  $\mathbb{Z}_N$ ) conditional on the first register being  $|1\rangle$  and inverse Fourier transforming the second register conditional on the first register being  $|0\rangle$ . In this new basis, the hidden subgroup state is

$$(9) \quad \rho_d = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} |\tilde{\phi}_{x,d}\rangle \langle \tilde{\phi}_{x,d}|$$

where

$$(10) \quad |\tilde{\phi}_{x,d}\rangle := \frac{1}{\sqrt{2}}(|0\rangle + \omega^{xd}|1\rangle)|x\rangle$$

with  $\omega := \exp(2\pi i/N)$ . When the subgroup is the trivial group, the standard approach produces a random state  $|t, x\rangle$  with  $t$  uniformly sampled from  $\mathbb{Z}_2$  and  $x$  uniformly sampled from  $\mathbb{Z}_N$ . Thus the hidden subgroup state when the hidden subgroup is  $\mathcal{H} = \mathcal{C}_1$  is simply the maximally mixed state

$$(11) \quad \rho_{\{e\}} = \frac{1}{N} \sum_{t \in \mathbb{Z}_2} \sum_{x \in \mathbb{Z}_N} |t, x\rangle \langle t, x| = \frac{I_{2N}}{2N}$$

where  $I_{2N}$  is the  $2N$ -dimensional identity matrix.

Our goal is to determine  $d$  given  $k$  copies of the state  $\rho_d$ . It will be helpful to write the state in a way that begins to reveal the connection to the subset sum problem. Note that we can write

$$(12) \quad \rho_d = \frac{1}{2N} \sum_{b,c \in \mathbb{Z}_2} \sum_{x \in \mathbb{Z}_N} \omega^{(b-c)xd} |b, x\rangle \langle c, x|.$$

Therefore

$$(13) \quad \rho_d^{\otimes k} = \frac{1}{(2N)^k} \sum_{b,c \in \mathbb{Z}_2^k} \sum_{x \in \mathbb{Z}_N^k} \omega^{[(b-c) \cdot x]d} |b, x\rangle \langle c, x|$$

$$(14) \quad = \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{p,q \in \mathbb{Z}_N} \omega^{d(p-q)} \sqrt{\eta_p^x \eta_q^x} |S_p^x, x\rangle \langle S_q^x, x|$$

where  $|S_r^x\rangle$  is the (normalized) uniform superposition over subsets of  $x \in \mathbb{Z}_N^k$  that sum to  $r \in \mathbb{Z}_N$ ,

$$(15) \quad |S_r^x\rangle := \frac{1}{\sqrt{\eta_r^x}} \sum_{b \in S_r^x} |b\rangle$$

with  $S_r^x := \{b \in \mathbb{Z}_2^k : b \cdot x = r\}$  denoting the set of bit strings corresponding to subsets of  $x$  that sum to  $r$ , and  $\eta_r^x := |S_r^x|$  denoting the number of such subsets. If  $\eta_r^x = 0$ , then no such state can be defined, and we use the convention  $|S_r^x\rangle = 0$ . When the subgroup is trivial,  $k$  copies of the

hidden subgroup state are simply  $k$  copies of the maximally mixed state,  $\rho_{\{e\}}^{\otimes k} = I_{(2N)^k} / (2N)^k$ .

#### 4. THE OPTIMAL MEASUREMENT

In this section, we present the optimal measurement for distinguishing the hidden subgroup states  $\rho_d^{\otimes k}$ . The measurement will have  $N$  outcomes, one for each possible value of  $d$ , and will be optimal in the sense that the probability of obtaining the correct outcome will be as large as possible. Recall that a general quantum measurement, a positive operator-valued measure (POVM), is specified by a set of positive operators  $\{E_j\}$ ,  $E_j \geq 0$ , that sum to the identity, i.e.,  $\sum_j E_j = I$ . Given a density matrix  $\rho$ , the probability of obtaining the outcome  $j$  is  $\text{tr } E_j \rho$ .

Ip was the first to consider optimal measurements for hidden subgroup problems [30]. In particular, he found the optimal measurement for the abelian hidden subgroup problem when the hidden subgroups are all given with equal a priori probabilities, thereby showing that the methods developed to solve the factoring problem are optimal. Ip also derived the optimal measurement for the dihedral hidden subgroup problem given a single copy of the hidden subgroup state. As we shall see, this measurement fails to efficiently identify the order two subgroups. Since we know that there exists a measurement for solving the DHSP using  $O(\log N)$  copies of the hidden subgroup states, it is of interest to understand the optimal measurement given  $k \gg 1$  copies.

The optimal measurement turns out to be the *pretty good measurement* (PGM) [25] (also known as the *square root measurement* or *least squares measurement*) [11].

To prove that the PGM is optimal, we will use the following theorem:

**Theorem 1** (Holevo [26], Yuen-Kennedy-Lax [48]). *Given an ensemble of quantum states  $\rho_i$  with a priori probabilities  $p_i$ , the measurement with POVM elements  $E_j$  maximizes the probability of successfully identifying the state if and only if*

$$(16) \quad \sum_i p_i \rho_i E_i = \sum_i p_i E_i \rho_i$$

$$(17) \quad \text{and} \quad \sum_i p_i \rho_i E_i \geq p_j \rho_j \quad \forall j.$$

This condition follows most easily from noting that the maximization problem is a semidefinite program [10, 30, 48]. While Theorem 1 provides necessary and sufficient conditions for a measurement to be optimal, it is non-trivial in general to construct measurements that satisfy these conditions.

Given  $\rho_d^{\otimes k}$  with equal a priori probabilities for each  $d \in \mathbb{Z}_N$ , we wish to find the measurements  $\{E_j\}_{j \in \mathbb{Z}_N}$  that maximize the probabilities of correctly identifying these states, where we identify the measurement outcome  $j$  with



our guess for the hidden subgroup label  $d$ . The PGM is given by

$$(18) \quad E_j = G^{-1/2} \rho_j^{\otimes k} G^{-1/2}$$

where the inverse is taken over the support of  $G$ , and where

$$(19) \quad G := \sum_{j \in \mathbb{Z}_N} \rho_j^{\otimes k}$$

$$(20) \quad = \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{p, q \in \mathbb{Z}_N} \sum_{j \in \mathbb{Z}_N} \omega^{j(p-q)} \sqrt{\eta_p^x \eta_q^x} |S_p^x, x\rangle \langle S_q^x, x|$$

$$(21) \quad = \frac{N}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} \eta_r^x |S_r^x, x\rangle \langle S_r^x, x|.$$

Inserting (14) and (21) into (18), we find that the pretty good measurement for the dihedral hidden subgroup states has the measurement operators

$$(22) \quad E_j = \frac{1}{N} \sum_{x \in \mathbb{Z}_N^k} \sum_{p, q \in \mathbb{Z}_N} \omega^{j(p-q)} |S_p^x, x\rangle \langle S_q^x, x|.$$

That this measurement is optimal can be seen by substitution into (16) and (17). We have

$$(23) \quad \sum_{i \in \mathbb{Z}_N} \rho_i E_i = \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{p, q \in \mathbb{Z}_N} \sqrt{\eta_p^x \eta_q^x} |S_p^x, x\rangle \langle S_q^x, x| = \sum_{i \in \mathbb{Z}_N} E_i \rho_i$$

which verifies (16). Now  $\rho_j$  is block diagonal with rank one blocks:  $\rho_j = \sum_{x \in \mathbb{Z}_N^k} |\rho_j^x, x\rangle \langle \rho_j^x, x|$  where

$$(24) \quad |\rho_j^x\rangle = \frac{1}{(2N)^{k/2}} \sum_p \omega^{jp} \sqrt{\eta_p^x} |S_p^x\rangle.$$

For any  $j \in \mathbb{Z}_N$  and for any block  $x \in \mathbb{Z}_N^k$ , we find

$$(25) \quad \langle \rho_j^x, x | \sum_{i \in \mathbb{Z}_N} \rho_i E_i | \rho_j^x, x \rangle = \frac{1}{(2N)^k} \sum_{p, q \in \mathbb{Z}_N} \eta_p^x \sqrt{\eta_p^x \eta_q^x}$$

$$(26) \quad \geq \frac{1}{(2N)^k} \sum_{p \in \mathbb{Z}_N} \eta_p^x = \langle \rho_j^x | \rho_j^x \rangle,$$

which verifies (17).

Notice that since  $G$  is not supported on the entire  $(2N)^k$ -dimensional space, the operators  $\{E_j\}_{j \in \mathbb{Z}_N}$  do not form a complete partition of the identity. (The dimension of the support of  $G$ ,  $\text{rank } G = |\{(x, p) : x \in \mathbb{Z}_N^k, p \in \mathbb{Z}_N, \eta_p^x > 0\}|$ , is given by Sloane's integer sequence A098966 [47].) To complete the measurement we can add an additional measurement operator,  $E_{\{e\}} := I - \sum_{j \in \mathbb{Z}_N} E_j$ . We associate this measurement outcome with the trivial subgroup. We emphasize that the measurement is only optimized for determining the order two subgroups. However, we will see that the optimal measurement with the additional measurement operator  $E_{\{e\}}$  also efficiently

identifies the trivial subgroup. Of course, the optimal measurement for the full dihedral group is never any better than the optimal measurement for distinguishing the order two subgroups.

## 5. SUCCESS PROBABILITY OF THE OPTIMAL MEASUREMENT

In this section we study the success probability of the optimal measurement for distinguishing the dihedral hidden subgroup states. Using the expressions (14) and (22), a simple calculation shows that the probability of successfully identifying an order two subgroup is independent of the hidden shift  $d$  and is given by

$$(27) \quad p := \text{tr } E_d \rho_d^{\otimes k} = \frac{1}{2^k N^{k+1}} \sum_{x \in \mathbb{Z}_N^k} \left( \sum_{r \in \mathbb{Z}_N} \sqrt{\eta_r^x} \right)^2.$$

We now show that the success probability has a sharp threshold as a function of the density  $\nu = k/\log N$ . More precisely, we find

**Theorem 2.** *If  $\nu \geq 1 + \frac{4}{\log N}$ , then the probability of successfully determining the order two subgroup is at least  $1/8$ . Furthermore, for any  $N$  and  $k$ , the probability of successfully determining the order two subgroup is less than  $2^k/N$  (which in particular is exponentially small in  $\log N$  for any fixed  $\nu < 1$ ).*

We will need the following lemma to prove the first statement of the theorem.

**Lemma 3** (Cf. proof of Lemma 4.1 of [41]). *For fixed  $r \in \mathbb{Z}_N$  and uniformly random  $x \in \mathbb{Z}_N^k$ ,*

$$(28) \quad \Pr \left( \eta_r^x \geq \frac{2^k - 1}{2N} \right) \geq 1 - \frac{4N}{2^k - 1}.$$

With this fact in hand, we can establish our main result.

*Proof of Theorem 2.* For the lower bound on the success probability, we have

$$(29) \quad p \geq \frac{1}{2^k N} \left( \frac{1}{N^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} \sqrt{\eta_r^x} \right)^2$$

by Cauchy's inequality applied to (27). Now by Lemma 3,

$$(30) \quad \frac{1}{N^k} \sum_{x \in \mathbb{Z}_N^k} \sqrt{\eta_r^x} \geq \sqrt{\frac{2^k - 1}{2N}} \Pr \left( \eta_r^x \geq \frac{2^k - 1}{2N} \right)$$

$$(31) \quad \geq \sqrt{\frac{2^k - 1}{2N}} - \sqrt{\frac{8N}{2^k - 1}}$$

for any  $r$ , which implies

$$(32) \quad p \geq \frac{N}{2^k} \left( \sqrt{\frac{2^k - 1}{2N}} - \sqrt{\frac{8N}{2^k - 1}} \right)^2$$

$$(33) \quad \geq \frac{2^k - 1}{2^{k+1}} - \frac{4N}{2^k}$$

$$(34) \quad \geq \frac{1}{4} - \frac{1}{2^k}$$

$$(35) \quad \geq \frac{1}{8}$$

where we have assumed  $k \geq \log N + 4$  (and also, in particular, we have used  $k \geq 3$ ).

For the upper bound on the success probability, we have

$$(36) \quad p \leq \frac{1}{2^k N^{k+1}} \sum_{x \in \mathbb{Z}_N^k} \left( \sum_{r \in \mathbb{Z}_N} \eta_r^x \right)^2$$

$$(37) \quad = \frac{2^k}{N}$$

where in the first line we have used the fact that the  $\eta$ 's are all integers to remove the square root in (27), and in the second line we have used the fact that  $\sum_{r \in \mathbb{Z}_N} \eta_r^x = 2^k$  for any  $x$ . This completes the proof.  $\square$

We claimed earlier that when the measurement identifies the order two subgroups with reasonable probability, it will also identify the trivial subgroup. This follows from a simple calculation: supposing  $\nu \geq 1 + \frac{4}{\log N}$ ,

$$(38) \quad p_{\{e\}} := \text{tr } E_{\{e\}} \rho_{\{e\}}^{\otimes k}$$

$$(39) \quad = 1 - \frac{\text{rank } G}{(2N)^k}$$

$$(40) \quad \geq 1 - \frac{N}{2^k}$$

$$(41) \quad \geq \frac{15}{16}.$$

## 6. BOUNDS BY INFORMATION-THEORETIC ARGUMENTS

The proof of the above threshold theorem used specific properties of the dihedral hidden subgroup problem. It is reasonable to ask if this is necessary, or if one could instead obtain the same bounds using the powerful techniques of quantum information theory. This appears not to be the case. Here we derive the information-theoretic lower bound  $\nu = k/\log N \geq p$ , which is weaker than the  $\nu \geq 1$  bound of Theorem 2 for probabilistic, non-exact algorithms.

Given  $k$  copies of the hidden subgroup state  $\rho_d$ , we want to determine the outcome  $d$  with success probability at least  $p$ . Viewed in a data transmission

setting, we can imagine a sender encoding  $\log N$  bits of information (the value  $d \in \mathbb{Z}_N$ ) in the quantum state  $\rho_d^{\otimes k}$ , after which a receiver decodes the  $\log N$  bits by solving the DHSP using the  $k$  copies of  $\rho_d$ . The number of copies  $k$  required for this approach to work can be analyzed with the tools of quantum information theory, thereby giving a lower bound on  $k$ . Because the amount of information received depends on the success probability  $p$ , the lower bound on  $k$  will also depend on  $p$ . Roughly speaking, the amount of information that can be transmitted with  $k$  copies is upper bounded by  $k$  bits, while the received amount of information is lower bounded by  $p \log N$ , leading to the lower bound  $k \geq p \log N$ . The details are as follows.

Given  $N$ , we define a *source*  $\mathcal{S}_k$  that draws from the uniform ensemble  $\{(1/N, \rho_d^{\otimes k})\}_{d \in \mathbb{Z}_N}$  where each  $d$  occurs with equal probability  $1/N$ . Holevo's  $\chi$  quantity, defined by

$$(42) \quad \chi(\mathcal{S}_k) := S\left(\frac{1}{N} \sum_d \rho_d^{\otimes k}\right) - \frac{1}{N} \sum_d S(\rho_d^{\otimes k})$$

where  $S(\cdot)$  denotes the Von Neumann entropy of a mixed quantum state [39], gives an upper bound on the accessible information of the ensemble. The state  $\rho_d$  is defined in a  $2N$ -dimensional Hilbert space, and its spectrum consists of the eigenvalues  $1/N$  and  $0$ , each with multiplicity  $N$ , while the spectrum of the mixture  $\frac{1}{N} \sum_d \rho_d$  consists of the eigenvalues  $1/N$  and  $0$ , each with multiplicity  $1$ , and the eigenvalue  $1/2N$  with multiplicity  $2N - 2$ . Hence, for the  $k = 1$  case, we have  $\chi(\mathcal{S}_1) = 1 - 1/N$ . For general  $k$ , we have  $S(\rho_d^{\otimes k}) = k \log N$  since the entropy is additive under tensor products. For the mixture  $\frac{1}{N} \sum_d \rho_d^{\otimes k}$  we note that the reduced density matrices of each copy are equal to  $\frac{1}{N} \sum_d \rho_d$ . Hence, by subadditivity of the Von Neumann entropy, the entropy of this mixture is bounded from above by  $k S(\frac{1}{N} \sum_d \rho_d)$ . Overall, this implies an upper bound of  $k(1 - 1/N)$  on the accessible information of  $\mathcal{S}_k$ .

Now, on the receiver's end, if the message can be decoded without error, then  $\mathcal{S}_k$  has a capacity of  $\log N$  bits per message. However, we should take into account that we are satisfied with a constant success probability  $p$ , which can be smaller than  $1$ . In this more general case, the information transmitted by the source will be bounded from below by  $I_p \geq \log N - H(p, \frac{1-p}{N-1}, \dots, \frac{1-p}{N-1})$ , where  $H(\cdot)$  is the Shannon entropy of a probability distribution. Since  $\chi(\mathcal{S}_k) \geq I_p$ , we find

$$(43) \quad k \left(1 - \frac{1}{N}\right) \geq \log N - H\left(p, \frac{1-p}{N-1}, \dots, \frac{1-p}{N-1}\right)$$

$$(44) \quad = \log N - (1-p) \log(N-1) - H(p, 1-p).$$

For constant  $p$  and large  $N$ , this converges to the lower bound  $k \geq p \log(N-1) - H(p, 1-p)$ , which is significantly weaker than the bound  $k \geq \log N$  from our earlier Theorem 2.

## 7. DETERMINING THE LEAST SIGNIFICANT BIT

Although the determination of the entire shift  $d$  requires at least  $\log N$  copies of the hidden subgroup state, one might hope to acquire partial information about the shift using fewer copies. For example, suppose one could determine the least significant bit of the shift using only a single hidden subgroup state. An iterative determination of the entire shift using such a measurement as a subroutine would still require  $\log N$  hidden subgroup states, but the basic measurement for determining a single bit would be much simpler. However, here we rule out such a possibility: the optimal measurement for determining even just a single bit of the shift still requires  $\log N$  hidden subgroup states. More precisely, we prove the following:

**Theorem 4.** *With  $k = \nu \log N$  copies of the dihedral hidden subgroup state  $\rho_d$ , the probability of successfully identifying the least significant bit of  $d$  is exponentially close to  $\frac{1}{2}$  for any fixed  $\nu < 1$ .*

Note that since there is a measurement to determine the entire shift with constant probability for any fixed  $\nu > 1$ , in particular there is a measurement to determine the least significant bit with probability bounded away from  $1/2$  in this regime. Thus Theorem 4 shows that the threshold for success remains essentially the same, at  $\nu \sim 1$ , for the problem of determining just the least significant bit.

To establish this result, we proceed as before: we first identify the optimal measurement, then derive an expression for its success probability, and finally place bounds on this expression. Our goal is to determine the least significant bit of  $d$ , i.e., whether  $d$  is even or odd. In other words, we would like to distinguish the two density matrices

$$(45) \quad \rho_{\pm} := \frac{2}{N} \sum_{d \text{ even, odd}} \rho_d^{\otimes k}.$$

Since  $\rho_+ + \rho_- = \frac{2}{N}G$  (with  $G$  given in (21)), the PGM for these states has the two POVM operators

$$(46) \quad E_{\pm} := \frac{N}{2} G^{-1/2} \rho_{\pm} G^{-1/2}$$

$$(47) \quad = \sum_{d \text{ even, odd}} E_d.$$

Now for simplicity, we assume  $N$  is even. The identity

$$(48) \quad \sum_{d \text{ even}} \omega^{d(p-q)} = \begin{cases} \frac{N}{2} & p = \pm q \\ 0 & \text{otherwise} \end{cases}$$

can then be used to simplify these expressions, and we obtain

$$(49) \quad \rho_{\pm} = \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} (\eta_r^x |S_r^x, x\rangle \langle S_r^x, x| \pm \sqrt{\eta_r^x \eta_{-r}^x} |S_r^x, x\rangle \langle S_{-r}^x, x|)$$

$$(50) \quad E_{\pm} = \frac{1}{2} \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} (|S_r^x, x\rangle \langle S_r^x, x| \pm |S_r^x, x\rangle \langle S_{-r}^x, x|).$$

We claim that this PGM is the optimal measurement for determining the least significant bit of the shift. To see this, check the conditions of Theorem 1. We have

$$(51) \quad \sum_{i \in \mathbb{Z}_N} \rho_i E_i = \rho_+ E_+ + \rho_- E_-$$

$$(52) \quad = \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} \left( \eta_r^x + \sqrt{\eta_r^x \eta_{-r}^x} \right) |S_r^x, x\rangle \langle S_r^x, x|$$

since the cross terms cancel. A similar calculation verifies (16). Then

$$(53) \quad \sum_{i \in \mathbb{Z}_N} \rho_i E_i - \rho_{\pm} = \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} \sqrt{\eta_r^x \eta_{-r}^x} (|S_r^x, x\rangle \langle S_r^x, x| \mp |S_r^x, x\rangle \langle S_{-r}^x, x|),$$

which is clearly a positive matrix, verifying (17).

The success probability of this optimal measurement is independent of whether  $d$  is even or odd, and is given by

$$(54) \quad \tilde{p} := \text{tr } E_+ \rho_+$$

$$(55) \quad = \frac{1}{2(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} \left( \eta_r^x + \sqrt{\eta_r^x \eta_{-r}^x} \right) \text{tr}(|S_r^x, x\rangle \langle S_r^x, x| + |S_r^x, x\rangle \langle S_{-r}^x, x|)$$

$$(56) \quad = \frac{1}{2} \left[ 1 + \frac{1}{(2N)^k} \left( \sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} \sqrt{\eta_r^x \eta_{-r}^x} + 2\eta_0^x + 2\eta_{N/2}^x \right) \right]$$

where we have used the fact that  $\sum_{x \in \mathbb{Z}_N^k} \sum_{r \in \mathbb{Z}_N} \eta_r^x = (2N)^k$ .

With these expressions in hand, we are ready to prove Theorem 4:

*Proof.* We bound the expression (56) for the success probability of the optimal measurement. First consider the cases  $r = 0, N/2$ . For  $r = 0$  we have

$$(57) \quad \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \eta_0^x = \frac{N^{k-1}(2^k - 1) + N^k}{(2N)^k}$$

$$(58) \quad \leq \frac{1}{N} + \frac{1}{2^k}$$

and for  $r = N/2$  we have

$$(59) \quad \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \eta_{N/2}^x = \frac{N^{k-1}(2^k - 1)}{(2N)^k}$$

$$(60) \quad \leq \frac{1}{N}.$$

In fact, the latter expression holds for any  $r \neq 0$ , since for any non-empty subset of numbers, specifying all but one of those numbers leaves exactly one possible subset summing to  $r$ . The additional  $N^k$  term for  $r = 0$  comes from the contribution of the empty set for each of the  $N^k$  possible assignments of the  $x$ 's.

For the remaining terms, we have

$$(61) \quad \frac{1}{(2N)^k} \sum_{r \neq 0, N/2} \sum_{x \in \mathbb{Z}_N} \sqrt{\eta_r^x \eta_{-r}^x} \leq \frac{1}{(2N)^k} \sum_{r \neq 0, N/2} \sum_{x \in \mathbb{Z}_N} \eta_r^x \eta_{-r}^x$$

$$(62) \quad = \frac{(N-2)(2^k-1)(2^k-2)N^{k-2}}{(2N)^k}$$

$$(63) \quad \leq \frac{2^k}{N}.$$

In the first line we have used the fact that the  $\eta$ 's are integers to remove the square root. In the second line we consider fixing one of the  $N-2$  values of  $r$ , and consider a non-empty subset  $S$  (of which there are  $2^k-1$ ) and a distinct non-empty subset  $T$  (of which there are  $2^k-2$ ). If we consider two elements  $i, j$  such that either  $i \in S - T$  and  $j \in T$ , or  $i \in T - S$  and  $j \in S$  (such a choice is always possible because  $S$  and  $T$  are non-empty and distinct), then for any values of the remaining  $k-2$  elements, there is exactly one choice for elements  $i$  and  $j$  such that the elements in  $S$  sum to  $r$  and the elements in  $T$  sum to  $-r$ . Thus the sum is exactly  $(N-2)(2^k-1)(2^k-2)N^{k-2}$ .

Using these expressions in (56), we find

$$(64) \quad \tilde{p} \leq \frac{1}{2} \left( 1 + \frac{2^k}{N} + \frac{6}{N} + \frac{3}{2^k} \right).$$

Thus we see that with  $k = \nu \log N$ , the success probability is exponentially close to  $1/2$  for any fixed  $\nu < 1$ .  $\square$

## 8. RELATION TO THE SUBSET SUM PROBLEM

Given that the optimal measurement solves the DHSP if (and only if)  $\nu > 1$ , we would like to understand whether this measurement can be implemented efficiently. In this section we consider how to implement the measurement by a quantum circuit, and we find that its implementation is closely related to the subset sum problem.

Recall the definition of the subset sum problem: given  $x \in \mathbb{Z}_N^k$  and  $t \in \mathbb{Z}_N$ , find a subset  $b \in \mathbb{Z}_2^k$  such that  $b \cdot x = t$ . If such a  $b$  exists, we call  $(x, t)$  a legal instance. In the decision version of the subset sum problem, we wish

to determine only whether a given instance is legal or not. This problem is NP-complete. We might also want to return one or more of the subsets  $b$  in the case where the instance is legal. Regev has shown that if there exists an efficient algorithm for finding one such subset for a large fraction of the legal instances, then one could solve the dihedral hidden subgroup problem efficiently [41]. More precisely,

**Theorem 5** (Regev [41]). *If there exists an efficient algorithm that finds a subset  $b$  such that  $b \cdot x = t$  for a fraction  $1/\text{poly}(\log N)$  of the legal subset sum instances  $(x, t)$  when  $k > \log N + 4$ , then there exists an efficient quantum algorithm for the dihedral hidden subgroup problem.*

Here we show a similar result for the implementation of the optimal measurement for the dihedral hidden subgroup states. Namely, if one can efficiently quantum sample from subset sum solutions at density  $\nu = k/\log N$ , then one can efficiently implement the optimal measurement for the DHSP with  $k$  copies. We also show a weak converse to this result: if one can efficiently implement the optimal measurement by a quantum circuit (under a certain restriction), then one can in turn solve the average case subset sum problem of corresponding density (and indeed, can quantum sample from subset sum solutions).

Recall from (22) that the POVM operators for the DHSP can be expressed as

$$(65) \quad E_j = \frac{1}{N} \sum_{x \in \mathbb{Z}_N^k} \sum_{p, q \in \mathbb{Z}_N} \omega^{j(p-q)} |S_p^x, x\rangle \langle S_q^x, x|$$

$$(66) \quad = \sum_{x \in \mathbb{Z}_N^k} E_j^x \otimes |x\rangle \langle x|$$

where

$$(67) \quad E_j^x := \frac{1}{N} \sum_{p, q \in \mathbb{Z}_N} \omega^{j(p-q)} |S_p^x\rangle \langle S_q^x|.$$

In other words, each  $E_j$  is block diagonal, with blocks labeled by some  $x \in \mathbb{Z}_N^k$ . Because each  $E_j$  has high rank, there is considerable freedom in how one implements the measurement by a quantum circuit. However, from a representation-theoretic perspective (see the Appendix), it is natural to perform this measurement in a particular way, first measuring the label  $x$  and then performing the POVM  $\{E_j^x\}_{j \in \mathbb{Z}_N}$  conditioned on that label. Note that each  $E_j^x$  is rank one, so that the POVM  $\{E_j^x\}_{j \in \mathbb{Z}_N}$  for fixed  $x \in \mathbb{Z}_N^k$  is refined into one-dimensional subspaces, removing much of the freedom in the implementation of the original POVM  $\{E_j\}$ .

For any given  $x \in \mathbb{Z}_N^k$ , we consider the implementation of the POVM  $\{E_j^x\}_{j \in \mathbb{Z}_N}$  by an  $x$ -dependent quantum circuit followed by a measurement in the computational basis to give the outcome  $j$ . In general, this circuit and measurement will act on a larger Hilbert space than is required to



hold the original input. The quantum circuit will then correspond to some unitary operation  $U^x$  on the larger space. Without loss of generality, we can assume that the final measurement is in a basis  $\{|j\rangle\}$  such that the values  $j \in \{0, 1, \dots, N-1\}$  indicate the measurement outcome  $E_j$ . According to Neumark's theorem, the unitary operator  $U$  has the block form

$$(68) \quad U^x = \begin{pmatrix} V^x & A^x \\ B^x & C^x \end{pmatrix}$$

where

$$(69) \quad V^x := \frac{1}{\sqrt{N}} \sum_{j,q \in \mathbb{Z}_N} \omega^{-jq} |j\rangle \langle S_q^x|$$

is a fixed  $(N \times 2^k)$ -dimensional matrix whose columns are the (subnormalized) vectors corresponding to the rank one POVM elements  $\{E_j^x\}$ , and  $A^x, B^x, C^x$  are arbitrary up to the requirement that  $U^x$  is unitary. It is convenient to perform a Fourier transform on the left, i.e., on the index  $j$  (over  $\mathbb{Z}_N$ , for the relevant values  $j \in \{0, 1, \dots, N-1\}$ ), giving a unitary operator

$$(70) \quad \tilde{U}^x = \begin{pmatrix} \tilde{V}^x & A^x \\ \tilde{B}^x & C^x \end{pmatrix}$$

with

$$(71) \quad \tilde{V}^x := \frac{1}{N} \sum_{j,p,q \in \mathbb{Z}_N} \omega^{j(p-q)} |p\rangle \langle S_q^x|$$

$$(72) \quad = \sum_{p \in \mathbb{Z}_N} |p\rangle \langle S_p^x|.$$

Clearly,  $U^x$  can be implemented equivalently if and only if  $\tilde{U}^x$  can be implemented efficiently. Therefore, if we have an efficient quantum circuit for the transformation

$$(73) \quad |p, x\rangle \mapsto \begin{cases} |S_p^x, x\rangle & \eta_p^x > 0 \\ |\psi_p^x\rangle & \eta_p^x = 0 \end{cases}$$

where  $|\psi_p^x\rangle$  is any state allowed by the unitarity of  $\tilde{U}^x$  (i.e., if we can efficiently quantum sample from subset sum solutions for legal inputs), then by running this circuit in reverse, we can efficiently implement  $\tilde{U}^x$ , and hence the measurement.

Conversely, given the ability to implement the optimal POVM by the measurement of  $x$  followed by an efficient implementation of  $U^x$ , we can solve the subset sum problem. By running the quantum circuit for  $\tilde{U}^x$  in the reverse direction, we can efficiently implement the transformation (73). Suppose we are trying to solve the subset sum problem for a legal instance  $(x, t)$ . Using (73), we can produce the state  $|S_t^x\rangle$ , which upon measurement gives a uniformly random subset of  $x$  summing to  $t$ . On the other hand, if

the instance is not legal, then we can easily check that the output does not correspond to a subset of  $x$  summing to  $t$ .

If we could efficiently implement the unitary operation  $\tilde{U}^x$  for any  $k = \text{poly}(\log N)$ , then we could solve the subset sum problem efficiently even in the worst case. Since the subset sum decision problem is NP-complete, such an implementation seems unlikely. However, for the purpose of solving the DHSP, it is sufficient to consider fixed  $k$  (as a function of  $N$ , with  $\nu = k/\log N > 1$  according to Theorem 2) and implement the measurement approximately. In this case, an implementation of the measurement only implies a solution to the average case subset sum problem at density  $\nu$ , which may be considerably easier. Conversely, to implement the measurement at density  $\nu$ , it is sufficient to approximately quantum sample subset sum solutions at that density.

The critical density  $\nu \sim 1$  for the success of the optimal measurement coincides with the critical density above which almost all subset sum instances are legal and below which almost all subsets have a distinct sum. No efficient algorithms are known for the subset sum problem at this critical density. But for sufficiently low or high density, the problem becomes tractable. For densities  $\nu < 0.941$ , there is an efficient algorithm assuming the ability to find short vectors in lattices [5, 7, 18, 35]. Unfortunately, this lattice problem seems to be difficult. However, using known basis reduction algorithms, this approach can be used to efficiently solve subset sum problems with no computational assumptions for very low density,  $k < c\sqrt{\log N}$  for some constant  $c$  [18, 35].

Since we require  $\nu > 1$  for a solution to the DHSP, the high density regime is more interesting for our purposes. Until recently, the best known result was a  $\text{poly}(k)$ -time algorithm for the case  $k > cN$  for some constant  $c$  [6, 19]. These results are not helpful since they yield algorithms whose running times are exponential in  $\log N$ . However, Flaxman and Pryzdatek recently showed how to produce subset sum solutions in  $\text{poly}(k)$  time with  $k = 2^{O(\sqrt{\log N})}$  [16]. Their result, together with Regev's connection to the subset sum problem (Theorem 5), gives an alternative subexponential time quantum algorithm for the DHSP with the same performance as Kuperberg's algorithm. However, it is not immediately clear whether their algorithm can be used to quantum sample (or even to randomly sample) from subset sum solutions, so it does not immediately provide an implementation of the optimal measurement.

It is not inconceivable that one could find a quantum algorithm (or even a classical one) for the subset sum problem at still lower density, and thus find an improved algorithm for the DHSP. Furthermore, we remark that our restriction of first measuring  $x$  and then implementing the appropriate measurement conditional on  $x$ , while natural from a representation-theoretic viewpoint, is not necessarily the best way to implement the optimal measurement. A direct implementation of the measurement without first measuring

$x$  could in principle produce a quantum algorithm for the DHSP without solving the subset sum problem.

## 9. DISCUSSION

In this paper we have studied the optimal measurement for distinguishing dihedral hidden subgroup states for order two subgroups. Using a result of Holevo and Yuen, Kennedy, and Lax, we proved that the pretty good measurement is optimal for this problem. We showed that the success probability of this measurement has a threshold around the critical density  $\nu \sim 1$ , and in particular, that  $\Omega(\log N)$  hidden subgroup states are necessary for the measurement to succeed with more than an exponentially small success probability. We also demonstrated that the problem of determining just the least significant bit of the answer is essentially no easier than the full problem. Finally, we considered the implementation of the measurement by a quantum circuit and found that it is closely related to the subset sum problem. We considered the special (but well-motivated) case in which the measurement first determines the block  $x$ , and then performs the optimal POVM within that block. For a given number of copies of the hidden subgroup state, we showed that this measurement can be implemented efficiently if and only if one can quantum sample from subset sum solutions at the corresponding density.

Many open questions remain. First, given Kuperberg's subexponential time algorithm for the DHSP using  $k = 2^{O(\sqrt{\log N})}$  copies of the hidden subgroup state, as well as the Flaxman-Pryzdatek algorithm for finding a subset sum solution at the corresponding density, it seems promising to look for an implementation of the optimal measurement by quantum sampling from subset sum solutions at this density. As an intermediate step, it would be interesting simply to find an algorithm for producing a subset sum solution uniformly at random.

Of course, implementing the optimal measurement at the Kuperberg density would not yield an improvement over previous algorithms, so it would be more interesting to find an implementation of the optimal measurement at still lower density. If one pursues the natural strategy of first measuring the block  $x$ , then our results show that this approach is at least as hard as solving the subset sum problem, in which case one could simply apply Regev's Theorem 5. However, as discussed above, one could consider implementing the optimal measurement without first measuring  $x$ , which might give an improved algorithm for the DHSP without yielding an algorithm for subset sum.

Finally, it would be interesting to consider optimal measurements for other non-abelian hidden subgroup problems. Can such measurements be implemented efficiently in any of the cases where efficient algorithms are already known? Or more ambitiously, can any new quantum speedups be found in

this way? Presumably the subset sum problem has some analog for other groups, and such a problem might be interesting in its own right.

#### ACKNOWLEDGMENTS

We thank Carlos Mochon and Frank Verstraete for helpful discussions of Theorem 1, and Abie Flaxman for correspondence regarding the algorithm in [16] and an earlier version thereof.

AMC received support from the National Science Foundation under Grant No. EIA-0086038, and was also supported in part by the Fannie and John Hertz Foundation, by the Department of Energy under cooperative research agreement DE-FC02-94ER40818, and by the National Security Agency and Advanced Research and Development Activity under Army Research Office contract DAAD19-01-1-0656. WvD was supported in part by the Cambridge-MIT Institute and by the Department of Energy under cooperative research agreement DE-FC02-94ER40818.

#### REFERENCES

- [1] M. Ajtai and C. Dwork, *A public-key cryptosystem with worst-case/average-case equivalence*, Proceedings of the 29th Annual ACM Symposium on Theory of Computing, 1997, pp. 284–293.
- [2] R. Beals, *Quantum computation of Fourier transforms over symmetric groups*, Proceedings of the 29th Annual ACM Symposium on Theory of Computing, ACM Press, New York, 1997, pp. 48–53.
- [3] E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM Journal on Computing **26** (1997), 1411–1473.
- [4] R. Boneh and R. Lipton, *Quantum cryptanalysis of hidden linear functions*, Advances in Cryptology – Crypto’95, Lecture Notes in Computer Science, vol. 963, Springer-Verlag, Berlin, 1995, pp. 424–437.
- [5] E. F. Brickell, *Solving low density knapsacks*, Advances in Cryptology – Crypto’83, Plenum Press, New York, 1984, pp. 25–37.
- [6] M. Chaimovich, G. Freiman, and Z. Galil, *Solving dense subset-sum problems by using analytical number theory*, Journal of Complexity **5** (1989), 271–282.
- [7] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C.-P. Schnorr, and J. Stern, *Improved low-density subset sum algorithms*, Computational Complexity **2** (1992), 111–128.
- [8] D. Deutsch and R. Jozsa, *Rapid solution of problems by quantum computation*, Proceedings of the Royal Society of London A **439** (1992), 553–558.
- [9] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London A **400** (1985), 97–117.
- [10] Y. C. Eldar, A. Megretski, and G. C. Verghese, *Designing optimal quantum detectors via semidefinite programming*, IEEE Transactions on Information Theory **49** (2003), 1007–1012.
- [11] ———, *Optimal detection of symmetric mixed quantum states*, IEEE Transactions on Information Theory **50** (2004), 1198–1207.
- [12] M. Ettinger and P. Høyer, *A quantum observable for the graph isomorphism problem*, arXiv:quant-ph/9901029.
- [13] M. Ettinger, P. Høyer, and E. Knill, *Hidden subgroup states are almost orthogonal*, arXiv:quant-ph/9901034.

- [14] ———, *The quantum query complexity of the hidden subgroup problem is polynomial*, Information Processing Letters **91** (2004), 43–48.
- [15] M. Ettinger and P. Høyer, *On quantum algorithms for noncommutative hidden subgroups*, Advances in Applied Mathematics **25** (2000), 239–251.
- [16] A. Flaxman and B. Przydatek, *Solving medium-density subset sum problems in expected polynomial time*, Proceedings of the 22nd Annual Symposium on Theoretical Aspects of Computer Science, Springer-Verlag, 2005, pp. 305–310.
- [17] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen, *Hidden translation and orbit coset in quantum computing*, Proceedings of the 35th Annual ACM Symposium on Theory of Computing, ACM Press, New York, 2003, pp. 1–9.
- [18] A. Frieze, *On the Lagarias-Odlyzko algorithm for the subset sum problem*, SIAM Journal on Computing **15** (1986), 536–539.
- [19] Z. Galil and O. Margalit, *An almost linear-time algorithm for the dense subset-sum problem*, SIAM Journal on Computing **20** (1991), 1157–1189.
- [20] D. Gavinsky, *Quantum solution to the hidden subgroup problem for Poly-Near-Hamiltonian groups*, Quantum Information and Computation **4** (2004), 229–235.
- [21] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani, *Quantum mechanical algorithms for the nonabelian hidden subgroup problem*, Combinatorica **24** (2004), 137–154.
- [22] L. Hales and S. Hallgren, *Quantum Fourier sampling simplified*, Proceedings of the 31st Annual ACM Symposium on Theory of Computing, ACM Press, New York, 1999, pp. 330–338.
- [23] ———, *An improved quantum Fourier transform algorithm and applications*, Proceedings of the 41st Annual Symposium on Foundations of Computer Science, IEEE, Los Alamitos, CA, 2000, pp. 515–525.
- [24] S. Hallgren, A. Russell, and A. Ta-Shma, *Normal subgroup reconstruction and quantum computing using group representations*, Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, ACM Press, New York, 2000, pp. 627–635.
- [25] P. Hausladen and W. K. Wothers, *A ‘pretty good’ measurement for distinguishing quantum states*, Journal of Modern Optics **41** (1994), 2385–2390.
- [26] A. S. Holevo, *Statistical decisions in quantum theory*, Journal of Multivariate Analysis **3** (1973), 337–394.
- [27] P. Høyer, *Efficient quantum transforms*, arXiv:quant-ph/9702028.
- [28] ———, *Conjugated operators in quantum algorithms*, Physical Review A **59** (1999), 3280–3289.
- [29] Y. Inui and F. Le Gall, *An efficient algorithm for the hidden subgroup problem over a class of semi-direct product groups*, arXiv:quant-ph/0412033.
- [30] L. Ip, *Shor’s algorithm is optimal*, 2003.
- [31] G. Ivanyos, F. Magniez, and M. Santha, *Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem*, International Journal of Foundations of Computer Science **14** (2003), 723–739.
- [32] J. Kempe and A. Shalev, *The hidden subgroup problem and permutation group theory*, Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, Philadelphia, 2005.
- [33] A. Kitaev, *Quantum measurements and the abelian stabilizer problem*, arXiv:quant-ph/9511026.
- [34] G. Kuperberg, *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, arXiv:quant-ph/0302112.
- [35] J. C. Lagarias and A. M. Odlyzko, *Solving low-density subset sum problems*, Journal of the ACM **32** (1985), 229–246.
- [36] C. Moore, D. N. Rockmore, A. Russell, and L. J. Schulman, *The power of basis selection in Fourier sampling: Hidden subgroup problems in affine groups*, Proceedings of

- the 15th Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, Philadelphia, 2004, pp. 1113–1122.
- [37] C. Moore and A. Russell, *The symmetric group defies strong Fourier sampling: Part II*, arXiv:quant-ph/0501066.
  - [38] C. Moore, A. Russell, and L. J. Schulman, *The symmetric group defies strong Fourier sampling: Part I*, arXiv:quant-ph/0501056.
  - [39] M. A. Nielsen and I. C. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.
  - [40] O. Regev, *A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space*, arXiv:quant-ph/0406151.
  - [41] ———, *Quantum computation and lattice problems*, Proceedings of the 43rd Annual Symposium on Foundations of Computer Science, IEEE, Los Alamitos, CA, 2002, pp. 520–529.
  - [42] ———, *New lattice based cryptographic constructions*, Proceedings of the 35th Annual ACM Symposium on Theory of Computing, 2003, pp. 407–416.
  - [43] M. Rötteler and T. Beth, *Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups*, arXiv:quant-ph/9812070.
  - [44] J. Serre, *Linear representations of finite groups*, Springer, New York, 1977.
  - [45] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing **26** (1997), 1484–1509.
  - [46] D. R. Simon, *On the power of quantum computation*, SIAM Journal on Computing **26** (1997), 1474–1483.
  - [47] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, 2004, <http://www.research.att.com/~njas/sequences>.
  - [48] H. Yuen, R. Kennedy, and M. Lax, *Optimum testing of multiple hypotheses in quantum detection theory*, IEEE Transactions on Information Theory **21** (1975), 125–134.

## APPENDIX: REPRESENTATION THEORY AND THE OPTIMAL MEASUREMENT

Many features of the hidden subgroup problem can be understood using simple group representation-theoretic arguments. Here we present such arguments and demonstrate their application to the DHSP.

Two important representations of a group  $\mathcal{G}$  for the HSP over that group are the left and right regular representations of  $\mathcal{G}$ . These representations act on a Hilbert space spanned by vectors  $\{|g\rangle\}_{g \in \mathcal{G}}$  as

$$(74) \quad D_L(g_1)|g_2\rangle = |g_1g_2\rangle \quad D_R(g_1)|g_2\rangle = |g_2g_1^{-1}\rangle.$$

Viewed as representations of the group algebra, these two representations are commutants of each other, i.e.,  $D_L(g_1)D_R(g_2) = D_R(g_2)D_L(g_1)$ . The hidden subgroup states  $\rho_{\mathcal{H}}$  defined in (3) commute with the left regular representation:  $D_L(g)\rho_{\mathcal{H}} = \rho_{\mathcal{H}}D_L(g)$  for all  $g \in \mathcal{G}$ . Hence, via Schur's lemma and the fact that the left and right regular representations are commutants, it is easy to show that a general hidden subgroup state can be expressed as

$$(75) \quad \rho_{\mathcal{H}} = \frac{1}{|\mathcal{G}|} \sum_{h \in \mathcal{H}} D_R(h).$$

The regular representations are reducible. Let  $\hat{\mathcal{G}}$  be a set of labels for a complete set of irreducible representations of  $\mathcal{G}$ , and for any  $x \in \hat{\mathcal{G}}$ , let  $\Gamma_x(g)$  be the  $x$ th irreducible representation (irrep) matrix for the group element

$g \in \mathcal{G}$ . Let  $d_x$  denote the dimension of the  $x$ th irrep. Then there exists a basis of the Hilbert space  $\{|g\rangle\}_{g \in \mathcal{G}}$ , labeled by  $|x, \ell, m\rangle$  with  $x \in \hat{\mathcal{G}}$  and  $\ell, m \in \mathbb{Z}_{d_x}$ , such that  $D_L$  and  $D_R$  act as

$$(76) \quad D_L(g) = \bigoplus_{x \in \hat{\mathcal{G}}} \Gamma_x(g) \otimes I_{d_x} \quad D_R(g) = \bigoplus_{x \in \hat{\mathcal{G}}} I_{d_x} \otimes \Gamma_x(g)$$

where  $I_d$  is the  $d$ -dimensional identity matrix. The unitary transformation that transforms between the bases  $\{|g\rangle\}_{g \in \mathcal{G}}$  and  $\{|x, \ell, m\rangle\}_{x \in \hat{\mathcal{G}}, \ell, m \in \mathbb{Z}_{d_x}}$  is nothing but the Fourier transform over  $\mathcal{G}$ ,

$$(77) \quad Q_{\mathcal{G}} := \frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} \sum_{x \in \hat{\mathcal{G}}} \sum_{\ell, m \in \mathbb{Z}_{d_x}} \sqrt{d_x} [\Gamma_x(g)]_{\ell, m} |x, \ell, m\rangle \langle g|.$$

Here  $[\Gamma_x(g)]_{\ell, m}$  is the matrix element in the  $\ell$ th row and  $m$ th column of the  $x$ th irrep at the group element  $g$ .

If we perform the quantum Fourier transform over  $\mathcal{G}$  on the state  $\rho_{\mathcal{H}}$ , we find in the new basis

$$(78) \quad \rho_{\mathcal{H}} = \frac{1}{|\mathcal{G}|} \bigoplus_{x \in \hat{\mathcal{G}}} I_{d_x} \otimes \left( \sum_{h \in \mathcal{H}} \Gamma_x(h) \right)$$

$$(79) \quad = \sum_{x \in \hat{\mathcal{G}}} p(x) \frac{I_{d_x}}{d_x} \otimes \rho_{\mathcal{H}, x} \otimes |x\rangle \langle x|,$$

a classical mixture over the irrep label  $x \in \hat{\mathcal{G}}$  with probabilities

$$(80) \quad p(x) := \frac{d_x}{|\mathcal{G}|} \sum_{h \in \mathcal{H}} \chi_x(h)$$

(where  $\chi_x := \text{tr } \Gamma_x$  denotes the character of the  $x$ th irrep) of a maximally mixed row state  $I_{d_x}/d_x$  and the column state

$$(81) \quad \rho_{\mathcal{H}, x} := \frac{1}{\sum_{h \in \mathcal{H}} \chi_x(h)} \sum_{h \in \mathcal{H}} \Gamma_x(h).$$

Since the row state is maximally mixed, it is clear that one learns nothing by measuring the row index [21]. Thus, it is natural to work in this basis and to discard the row state, focusing on the column state  $\rho_{\mathcal{H}, x}$ . This procedure corresponds exactly to the particular form of the optimal POVM considered in Section 8.

To see this correspondence in detail for the DHSP, consider the irreducible representations of the dihedral group [44]. These irreps are all either one- or two-dimensional. The two-dimensional irreps may be conveniently labeled by an integer  $1 \leq x \leq \lceil N/2 \rceil - 1$ , and are given by

$$(82) \quad \Gamma_x(s^k) = \begin{pmatrix} \omega^{xk} & 0 \\ 0 & \omega^{-xk} \end{pmatrix} \text{ and } \Gamma_x(rs^k) = \begin{pmatrix} 0 & \omega^{-xk} \\ \omega^{xk} & 0 \end{pmatrix}$$

where  $\omega := \exp(2\pi i/N)$ . Notice that the irreps satisfy  $\Gamma_{-x}(g) = X\Gamma_x(g)X$  where  $X$  is the Pauli matrix

$$(83) \quad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

When  $N$  is odd, there are two one-dimensional irreps, the trivial irrep

$$(84) \quad \Gamma_\tau(s^k) = \Gamma_\tau(rs^k) = 1$$

and the alternating irrep

$$(85) \quad \Gamma_\sigma(s^k) = 1 \text{ and } \Gamma_\sigma(rs^k) = -1.$$

When  $N$  is even, there are two additional one-dimensional irreps, the even irrep

$$(86) \quad \Gamma_e(s^k) = \Gamma_e(rs^k) = (-1)^k$$

and the odd irrep

$$(87) \quad \Gamma_o(s^k) = (-1)^k \text{ and } \Gamma_o(rs^k) = -(-1)^k.$$

Now consider the approach to the DHSP of first performing a quantum Fourier transform over  $\mathcal{G} = \mathcal{D}_N$  and then measuring the irrep index. If the result obtained corresponds to a two-dimensional irrep, then we can measure the row index and will randomly obtain one of two outcomes. We associate one of these outcomes with the irrep label  $x$  and the other with the irrep label  $-x$ , performing the  $X$  operation on the column in the latter case. Furthermore, we group the trivial irrep and the alternating irrep together into a two-dimensional space, and similarly for the even and odd irreps. Labeling these two spaces 0 and  $N/2$ , respectively, it is now easy to see that this procedure is equivalent to the measurement procedure outlined in Section 8, where the irrep label  $x$  corresponds to the measurement of  $x \in \mathbb{Z}_N$ .

SANTA FE INSTITUTE, SANTA FE, NM 87501, USA

*E-mail address:* `dabacon@santafe.edu`

INSTITUTE FOR QUANTUM INFORMATION, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CA 91125, USA

*E-mail address:* `amchilds@caltech.edu`

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, SANTA BARBARA, CA 93106, USA

*E-mail address:* `vandam@cs.ucsb.edu`